Why you should care about glexec

Hint: It's about security

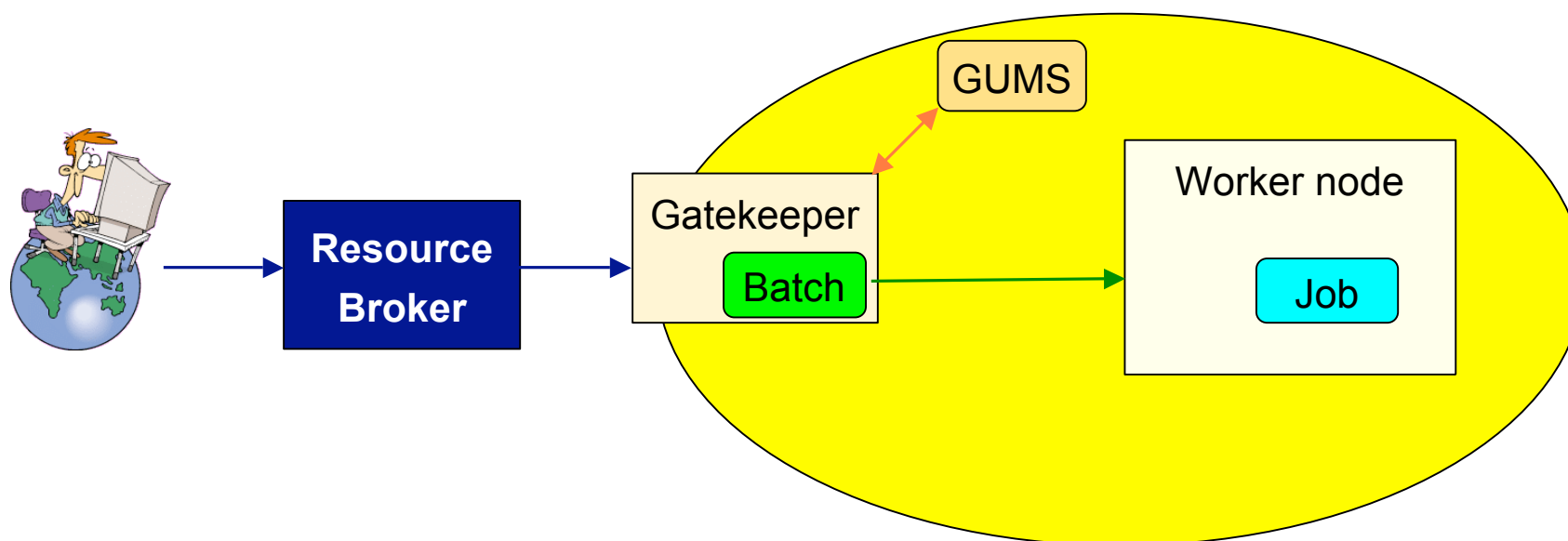## OSG Site Administrator's Meeting

Written by Igor Sfiligoi
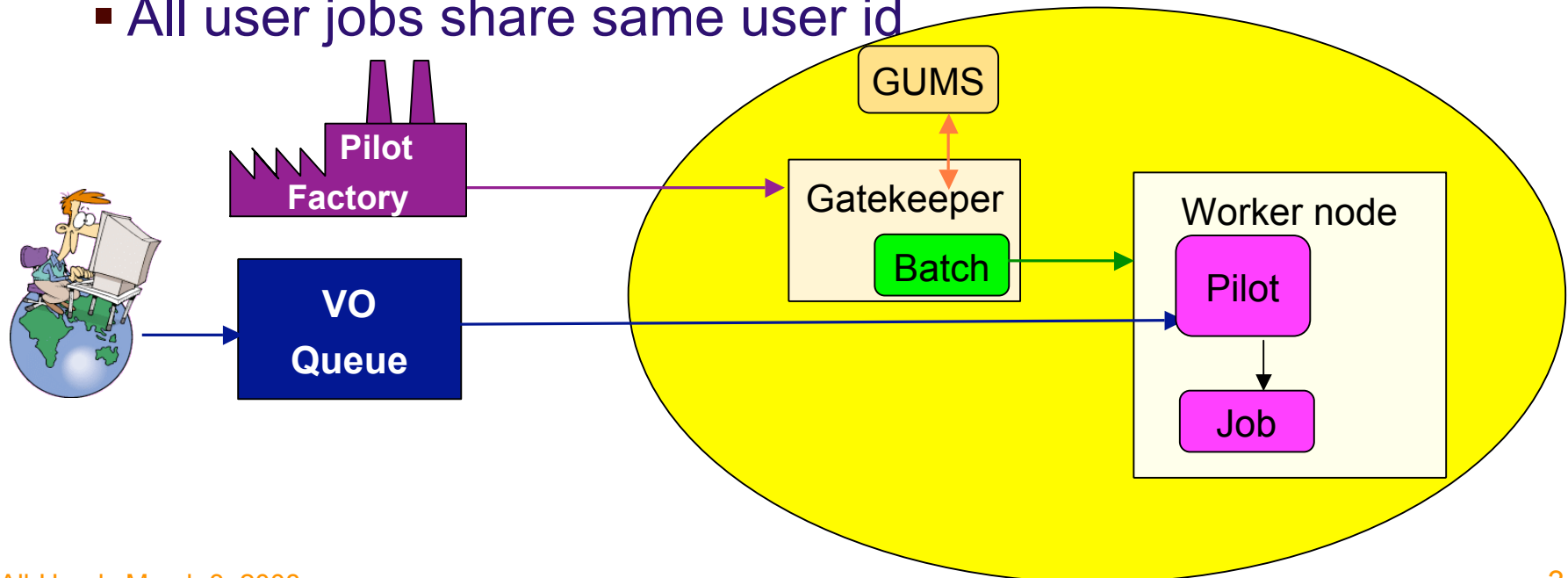Presented by Alain Roy

Traditional Grid Jobs

- ## User jobs come through the gatekeeper
  - You see all jobs come in
  - You ensure they run as the correct user
  - You can do accounting

Pilot Grid Jobs

- User jobs **don't** come through the gatekeeper
  - Only pilots enter via gatekeeper
  - Each pilot accepts work from VO
  - You don't see user jobs
    - No local authorization, no accounting
    - All user jobs share same user id

Pilot user jobs share user ids!

- Hey, mind if I borrow your proxy?
- Oops, was that your file?

- gLExec will solve this problem

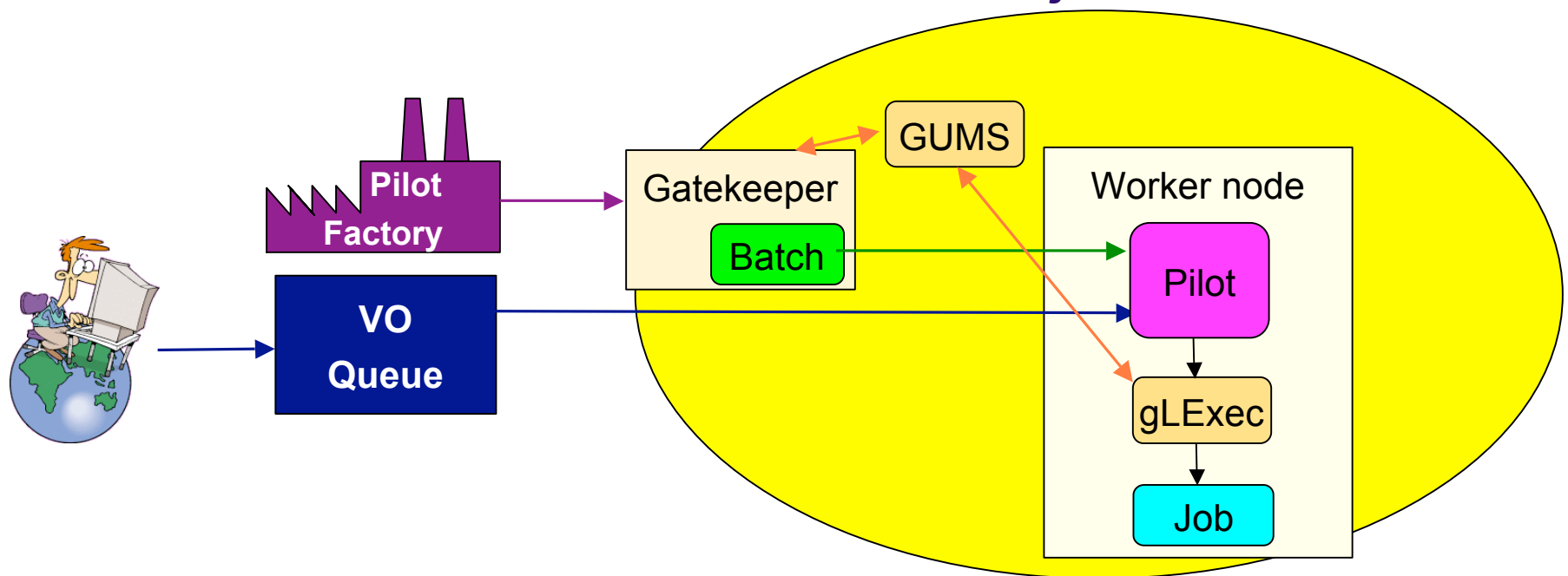# Pilot jobs are in use today

Open Science Grid

- Two VOs are actively using Pilot jobs
  - CDF
  - ATLAS
- Others are about to start using them
  - CMS
  - MINOS
- Pilot jobs are here to stay

Pilot Grid Jobs with gLExec

Open Science Grid

- ## User jobs started using gLExec
  - Authorized with local authorization tools (GUMS)
  - Correct user ID used to start job

What is gLExec

- A Grid-aware suExec derivative
  - Allows execution of commands as a different user
  - Authorization and mapping based on X.509 proxy
- A privileged executable (setuid to root)
  - Needed to switch identities
- Pluggable architecture
  - PRIMA/GUMS plugin used by default in OSG

gLExec IS a privileged executable

- gLExec is NOT a privileged service
  - Not listening on any network port
- gLExec is a privileged executable
  - Will run as root at least part of the time
  - A bug can potentially give an attacher root privileges
- gLExec has been audited by EGEE for potential security problems
  - None have been found

gLExec and accounting

- gLExec keeps detailed logs of each invocation, including
  - user DN and FQAN
  - start and stop times
  - process id
- A gLExec GRATIA probe exists for automatic accounting extraction
  - but logs are also human readable

gLExec and Pilots

- Pilots cannot be forced to use gLExec
  - Pilots need to be gLExec-aware
- But if gLExec is installed, site can require its use by *policy*
- Using gLExec is in the best interest of pilots
  - Protects them from malicious users (UID switching)

gLExec installation

- gLExec supported by OSG
  - distributed via VDT

- Needs to be installed on all the worker nodes

- Requires host certificate or service proxy to talk to GUMS

  For more details, see talk in the "Configuring OSG" session

Conclusions

- **Pilot jobs are gaining momentum**
  - Most big VOs (do or will) use them
- **gLExec helps restore security for pilot jobs**
- **It is a privileged executable**
  - But security benefits overweight risks
- **Supported by OSG**
  - Distributed in VDT